F

Firewall: Types, Rules, Network Placement, and Limits

A firewall enforces a traffic policy between systems or networks. Learn the main firewall types, rule design, placement, logging, and limitations.

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
4 min

CONTENTS

In this guide

01 How a firewall works
02 Common firewall types
03 Where firewalls are placed
04 How to write safer rules
05 Common configuration mistakes
06 What a firewall cannot do
07 Sources

Quick answer: A firewall is a hardware, software, or cloud control that allows or blocks network traffic according to a policy. It can reduce exposed services, segment networks, and record connection attempts. A firewall does not remove malware, repair vulnerable

software, or automatically make allowed traffic trustworthy.

For an example of network placement, a screened subnet firewall separates public-facing services into a DMZ. The useful question is which flows each boundary permits, not simply whether the diagram contains more than one firewall.

01 How a firewall works

Network traffic is divided into packets. A firewall evaluates selected information—such as source and destination address, protocol, port, connection state, application, identity, or content—and compares it with ordered rules. The action may be allow, deny, reject, log, inspect, or route to another security service.

A policy should start with business communication needs, not a collection of vendor defaults. The safest general pattern is to deny traffic that is not explicitly required, while documenting necessary exceptions and testing the operational impact.

02 Common firewall types

- **Packet-filtering firewall:** makes decisions primarily from network and transport headers such as IP address, protocol, and port.
- **Stateful firewall:** tracks active connections and can allow returning packets that belong to an established session.
- **Application proxy:** terminates a connection and creates a separate connection to the destination, allowing application-aware controls.
- **Next-generation firewall:** combines stateful filtering with application identification and may include intrusion prevention, identity, or content inspection.
- **Web application firewall:** specializes in HTTP traffic to web applications. It is not a replacement for a general network firewall or secure application code.
- **Cloud firewall or firewall service:** applies policy to cloud networks or routes traffic through a provider-managed inspection point.

- **Host firewall:** runs on one endpoint. For device-specific profiles and inbound/outbound rules, see Personal Firewall.

03 Where firewalls are placed

Firewalls can protect an internet edge, a data-center boundary, cloud subnets, an office, a development environment, or an individual workload. Internal segmentation limits lateral movement between user devices, servers, management systems, and operational technology. Public services are often placed in a demilitarized zone so compromise does not provide a direct path to backend systems.

Placement determines visibility. An encrypted session may hide application content unless inspection is configured, while traffic that never crosses the enforcement point cannot be filtered there.

04 How to write safer rules

1. Identify the exact application, owner, source, destination, protocol, port, direction, environment, and business reason.
2. Use the narrowest practical scope. Avoid permanent any-source, any-destination, or any-service rules.
3. Put specific rules before broader ones when the platform evaluates rules in order, and understand its implicit default action.
4. Set an owner and review or expiry date for temporary exceptions.
5. Log denied traffic and high-risk allowed flows without collecting unnecessary sensitive content. Send important logs to a protected central system.
6. Test from the intended source and also verify that unintended sources remain blocked.

05 Common configuration mistakes

Frequent problems include exposing management interfaces to the internet, trusting an entire internal network, leaving obsolete rules after a project ends, permitting broad outbound access, disabling logging, and treating address translation as a security policy. Another mistake is opening a port when the application is listening on every interface or has weak authentication.

06 What a firewall cannot do

A firewall cannot patch the service behind an allowed port, stop a user from entering credentials on an allowed phishing site, or reliably identify all malware inside encrypted or permitted traffic. Application inspection can improve visibility but creates performance, privacy, certificate, and compatibility considerations. Administrators or malware with sufficient control may also alter a host firewall.

Use firewalls with secure configuration, patching, identity controls, endpoint protection, application security, backups, monitoring, and incident response. Review the policy after architectural and business changes, not only after an incident.

07 Sources

Firewall categories and policy principles follow NIST SP 800-41 Revision 1. Segmentation guidance is also reflected in CISA hardening guidance.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com